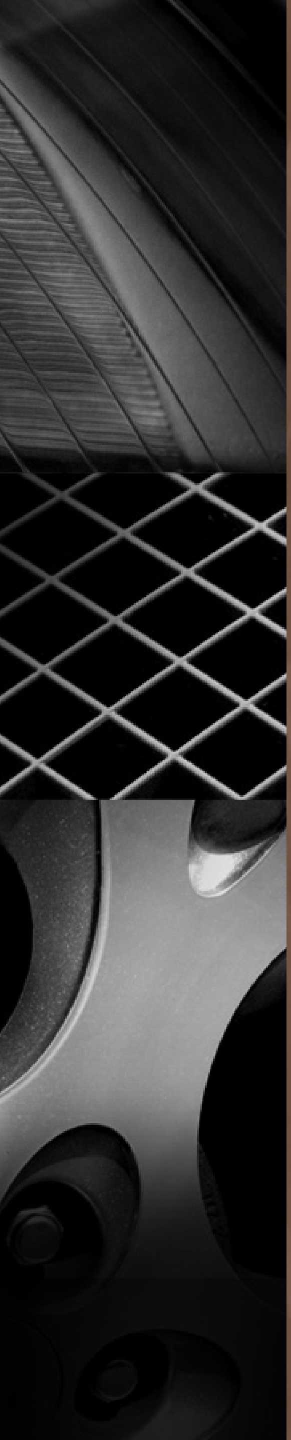
Real World Mobile Forensics

The Intersection of Research, Academia, and Case Work

Daren Melson



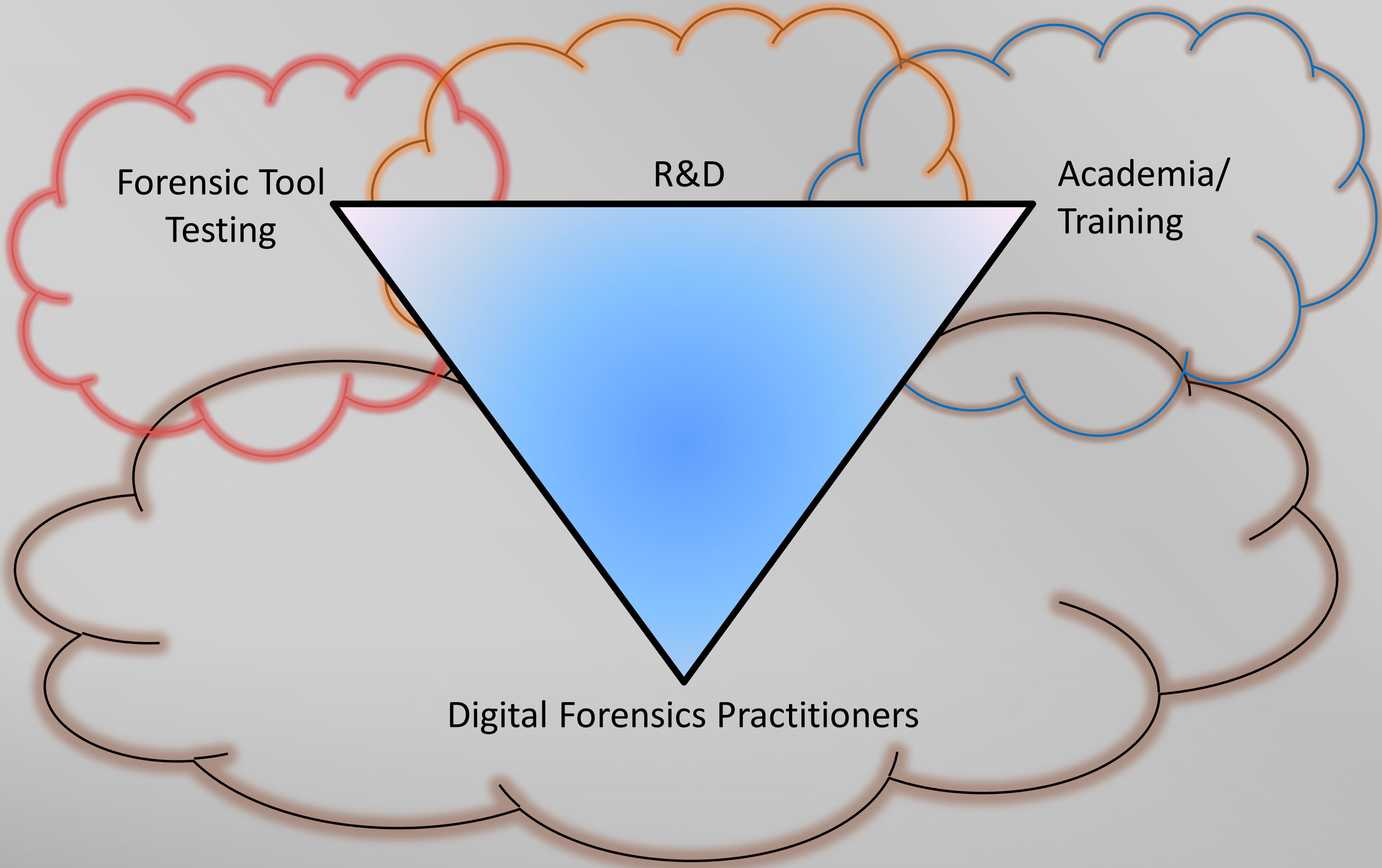
Part I: The Symbiotic Relationship

Academia, Research, and Practice

Part II: A Look at a Few Cases

The Evolution of Technique - What Worked and What Didn’t

The Symbiotic Relationship



Forensic Tool Testing

R&D

Academia/ Training

Digital Forensics Practitioners

A Look at Some Cases

- Keeping in mind the importance of, and the nature of, the relationships we just discussed within the Mobile Forensics Community, let's look at some ways in which "the rubber meets the road".

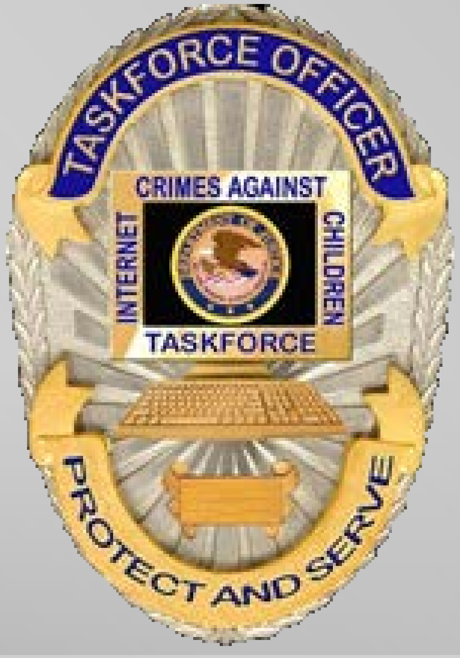
- Because of the ubiquity of cell phone usage, Mobile Forensics has the potential to play a part in every type of Law Enforcement or Civil case imaginable.

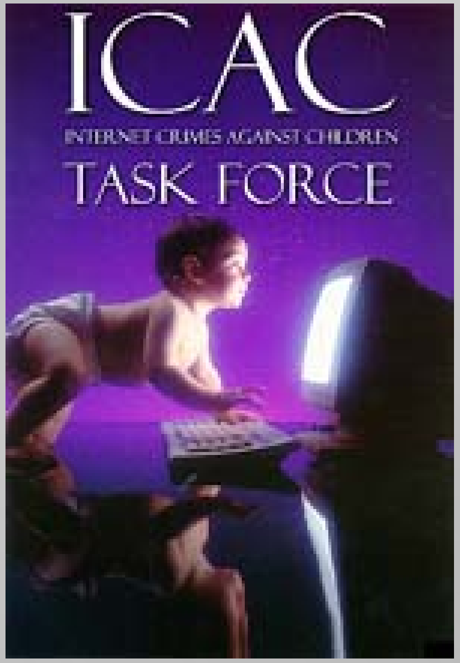
Establishing A Subject’s Location

- Cell Tower Records
  - Missing persons case
  - Computer examination yielded nothing solid
  - Body found; now a homicide case gone “cold”
  - Cell tower records solved the case
- Geolocation Data
  - Victim was shot during gang activity
  - Subject swore he wasn’t there
  - Deleted video taken at time of shooting
  - Geolocation data solved the case

Crimes Against Children Investigations

- A large number of Law Enforcement practitioners in the mobile/digital forensics community have a majority of their caseload come from the epidemic of child pornography and the exploitation of minors.
- Many mobile forensics cases center around the recovery of deleted material.
  - Deleted Videos
  - Deleted Images
  - Deleted Emails
  - Deleted Texts



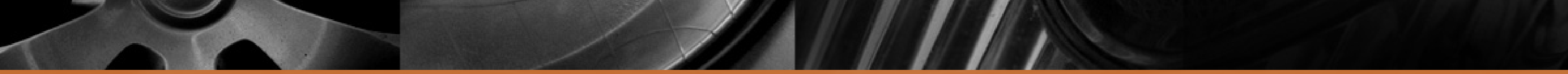


Crimes Against Children Investigations

- A child swore that her stepfather was abusing her and that he would video the alleged molestation with his cell phone.
- The stepfather denied the allegations and willingly turned over his phone for examination.
- The local PD examiner used a popular tool but the only videos he found were benign.
- In subsequent interviews with the investigators the girl continued to stick to her story.
- A manual file carving examination of the physical image of the phone uncovered 108 deleted video files; proving the child’s allegations.

Illegal Interception of Communications

- Many cases involve the potentially illegal interception of communications through the use of spyware or other means.
- Sometimes its just a “wild goose chase” . . .
- One person amazingly knew intimate details about their business partner that the victim swore had only been spoken to the confidentiality of his attorney.
- The attorney and his client both suspected an illegal interception of communications was taking place so they turned over the client’s phone and computer for examination.
- Examination of the phone, and the computer it had been synced to, uncovered evidence of installed spyware.



Future Expectations

- Standardization is desperately needed among mobile devices – connectors, data storage, etc. However, until such time that the mobile device industry begins to adopt standards, the forensic community will have to remain FLEXIBLE in their tools and techniques, as they seek to find the data.
- I expect that mobile devices will continue to proliferate in quantity and capacity, continuing to move forward at a “blistering pace”. Sadly, I also expect that mobile forensics tools and techniques will continue to lag behind.
- In the business sector, many corporations are adopting BYOD policies. These policies will cause a massive surge in mobile phone forensics cases – corporate forensics teams will be quickly inundated with all manner of mobile devices for examination.
- Given that today many people use smart phones more than computers, I expect that mobile device forensics will become the major focus of the digital forensics world in the very near future.